



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/549,396	04/14/2000	Pankai Rohatgi	YOR9-1999-0229-US2	8212

7590 11/05/2003

Louis P Herzberg
Intellectual Property Law Dept
IBM Corporation
P O Box 218
Yorktown Heights, NY 10598

EXAMINER

ARANI, TAGHI T

ART UNIT	PAPER NUMBER
----------	--------------

2131

2

DATE MAILED: 11/05/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/549,396

Applicant(s)

ROHATGI, PANKAI

Examiner

Taghi T. Arani

Art Unit

2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 14 April 2000.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-44 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-10, 15, 17, 18, 20, 21, 23-29 and 31-44 is/are rejected.
- 7) ☐ Claim(s) 11-14, 16, 19, 22 and 30 is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
- Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- 11) ☐ The proposed drawing correction filed on _____ is: a) ☐ approved b) ☐ disapproved by the Examiner.
- If approved, corrected drawings are required in reply to this Office action.
- 12) ☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

- 13) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.
- 14) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).
- a) ☐ The translation of the foreign language provisional application has been received.
- 15) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892) 4) ☐ Interview Summary (PTO-413) Paper No(s). _____
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948) 5) ☐ Notice of Informal Patent Application (PTO-152)
- 3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ 6) ☐ Other: _____

DETAILED ACTION

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title

Claims 23-28, 36-40 are rejected under 35 U.S.C. 101 because claim 23 recites a method comprising: “ generating a TCR commitment opening function for extracting a data string committed to by at least one TCR commitment message, utilizing a corresponding TCR opening string....., and employing a TCR function and a regular commitment scheme used in generatingTCR commitment message and used in generating corresponding TCR opening string”. Steps of claim 23 is merely a series of function applied on various strings or messages with no concrete and tangible result.

Dependent claims 32-34 are also rejected by virtue of their dependencies.

Apparatus claims 24-25 corresponding to method claims 23 are also rejected for the same reasons stated above.

Dependent claims 26-28, 36-40 are also rejected by virtue of their dependencies.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 26-28, 31 and 37-40 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 26 recites the limitation "said regular commitment scheme" in lines 20-21. There is insufficient antecedent basis for this limitation in the claim. Dependent claims 27-28 and 39 are rejected by virtue of their dependencies.

Claims 26-28, 37-40 are method claims depending from an apparatus claim 25 (computer program product). Dependent method claim should not be depending from a base method claim.

Claims 31 and 35 recite "any TCR function" and "any regular commitment". The terms "any TCR function" and "any regular commitment" are not determinant and are relative terms which renders the claim indefinite. The specification does not provide a standard for ascertaining the requisite degree, and one of ordinary skill in the art would not be reasonably apprised of the scope of the invention.

Dependent claims 41-43 are rejected by virtue of their dependencies.

Double Patenting

The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. See *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and, *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent is shown to be commonly owned with this application. See 37 CFR 1.130(b).

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

Claims 1-9, 15, 17-18, 20 and 21 are provisionally rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claims 1, 6, 12, 13, 14, 18, 46 and 60 of copending Application No. 09/307,493. Although the conflicting claims are not

identical, they are not patentably distinct from each other because claim 1 of the copending application '493 is directed to a method of generating a signature for a message employing a public/private key pair in which the private key includes at least one enhancing key; and a public key which includes a TCR commitment (or a regular commitment recited in claim 12 of the Application '493) to at least one enhancing key recited in **claims 1 and 3** of the pending application, see claim 1, lines 4-6.

Claim 1 of the copending application '493 recites a public key which includes a TCR commitment to at least one enhancing key. That is, a public key comprises "a commitment to an enhancing key" recited in **claim 2** of the pending application.

Claim 6 of the copending application '493 recites inclusion of certificate in the signed message. That is, a certificate for the public key recited in **claim 6** of the pending application.

Claim 1 of the copending application discloses that the commitment is a TCR commitment recited **claim 7** of the pending application.

Claim 1 of the copending application '493 is directed to a signature for a message employing a key pair in a commitment (i.e. TCR commitment scheme) base signature recited in **claim 20** of the pending application.

Claims 46 and 60 of copending application '493 discloses computer program code and apparatus corresponding to **claims 9 and 15** of the pending application.

Claim 14 of the copending application '493 discloses a bound (i.e. 36-time key pair) number of times recited in **claims 17 and 18**.

Claims 12-14 of the application '493 discloses a commitment based signature employing TCR-commitment to an enhancing key implemented (i.e. in a process) for a 36-time key pair (i.e. performing hash calculation) corresponding to recited limitations of **claims 4 , 5 and 8**.

Claim 14 of the copending application '493 discloses employing commitment based signature scheme implementing for a 36-time key pair. That is, a 36-time signature scheme recited in **claim 21**.

This is a provisional obviousness-type double patenting rejection because the conflicting claims have not in fact been patented.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.

Claims 10⁴⁴ and 29 are rejected under 35 U.S.C. 102(a) as being anticipated by M.

Belare , P. Rogaway, Collision-Resistant Hashing: Towards making UOWHFs Practical,
Department of Computer Science & Engineering, University of California at San Diego, July
1997.

Belare teaches a signing with an TCR Hash family where the signing algorithm chooses K (i.e. a commitment) anew for each message (i.e. a first string). Belare further teaches that the key K is included with the signature. That is a second TCR function is applied to a second string that includes the commitment (i.e. key K), see pages 26-27, see also page 28. Belare discloses

Art Unit: 2131

the steps of verifying a message using TCR function (i.e. a TCR de-commitment function) for verifying the TCR commitment message generated , see page 26.

Claim 44 is an apparatus corresponding to method claim 29. It is rejected for the same reasons stated in the statement of rejection of claim 29 above.

Allowable Subject Matter

Claims 11-14, 16,19 , 22 and 30 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Conclusion

Any inquiry concerning this communication or earlier communications from examiner should be directed to Taghi Arani, whose telephone number is (703) 305-4274. The examiner can normally be reached Monday through Friday from 8:00 AM to 5:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh, can be reached at (703) 305-9648. The Fax numbers for the organization where this application is assigned are:


After-final (703) 746-7238

Official (703) 746-7239

Non-Official/Draft (703) 746-7240

Taghi Arani

Patent Examiner


AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2106